Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi) eISSN 2527 - 4902
Vol. 22 No. 2, Desember 2020: 143 - 158

Studi Kebijakan Perlindungan Data Pribadi dengan *Narrative Policy Framework*: Kasus Serangan Siber Selama Pandemi Covid-19

A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic

Ratnadi Hendra Wicaksana[1], Adis Imam Munandar[2], Palupi Lindiasari Samputra[3]
[1,2,3]*Master Degree Program in Intelligence Studies, School of Strategic and Global Studies,*
Universitas Indonesia (UI)
Jalan Salemba Raya No 4 Jakarta, Indonesia

[1]ratnadi.hendra@ui.ac.id, [2]adis.imam@ui.ac.id, [3]palupi.ls@ui.ac.id

Naskah diterima: 16 November 2020 direvisi: 23 November 2020, disetujui: 7 Desember 2020

Abstract

The Covid-19 pandemic has provided opportunities for cyber criminals to increase the intensity of their attacks. As a result, the security of personal data is threatened. This study analyzed personal data protection policies using the Narrative Policy Framework (NPF) method. In this analysis, benchmarking approach was carried out to learn United Kingdom and Malaysia's best practices in developing personal data protection policies, especially in new normal context. The aim is to obtain policy solutions to strengthen data security protection in Indonesia in the face of cyber attacks in the new normal period. The results showed that hero character is found in a comprehensive personal data protection regulation that has long been implemented by United Kingdom and Malaysia. In Indonesia, the fictional hero does not play a major role because of fictional villain, which is represented by lack of integrated regulation for the protection of personal data from the threat of cyber attacks. The victims of the villain are personal and industrial data security. Based on this, the policy solutions that need to be taken are: (1) speeding up the ratification of the Personal Data Protection, (2) providing special regulations dealing with cybersecurity and cyber criminal crimes, (3) building a cross-sectoral cybersecurity management ecosystem, (4) increasing awareness and human resources capacity related to cybersecurity.

Keywords*: policy, personal data protection, cyber attack, new normal, Covid-19 pandemic.*

Abstrak

Pandemi Covid-19 telah memberikan peluang bagi para penjahat siber untuk meningkatkan intensitas serangannya. Akibatnya, keamanan data pribadi menjadi terancam. Penelitian ini melakukan analisis kebijakan perlindungan data pribadi melalui metode Narrative Policy Framework (NPF). Di dalam analisis ini dilakukan benchmarking antara kebijakan perlindungan data pribadi di Indonesia dengan best practice di Inggris Raya dan Malaysia, khususnya dalam situasi new normal. Tujuannya untuk mendapatkan solusi kebijakan yang memperkuat perlindungan keamanan data pribadi di Indonesia dalam menghadapi serangan siber di masa new normal. Hasil penelitian menunjukkan adanya karakter hero,

dalam bentuk regulasi komprehensif tentang perlindungan data pribadi yang telah lama diterapkan oleh Inggris Raya dan Malaysia. Di Indonesia, peran dari karakter hero belum cukup kuat karena adanya villain dalam bentuk ketiadaan regulasi terpadu untuk perlindungan data pribadi dari ancaman serangan siber. Victim dari villain tersebut adalah keamanan data pribadi dan data pelaku industri. Berdasarkan hal tersebut, maka kebijakan yang dapat diambil adalah: (1) mempercepat pengesahan RUU perlindungan data pribadi, (2) menyediakan regulasi khusus yang menangani keamanan siber dan kejahatan kriminal siber, (3) membangun ekosistem penanganan keamanan siber lintassektor, (4) meningkatkan kesadaran dan kapasitas SDM terkait keamanan siber.

Kata kunci: kebijakan, perlindungan data pribadi, serangan siber, *new normal*, pandemi Covid-19.

PENDAHULUAN

Pandemi Covid-19 telah menjadi bencana global yang cepat menyebar luas dan menyebabkan krisis kesehatan maupun ekonomi di berbagai belahan dunia. Berdasarkan laporan dari situs resmi yang dikeluarkan World Health Organization (WHO) (https://covid19.who.int), jumlah kasus terkonfirmasi positif Covid-19 per 14 November 2020 telah mencapai 53.164.803 jiwa di seluruh dunia. Sebagai tindak lanjut pandemi tersebut, pemerintah di berbagai negara menerapkan *lockdown* dengan tujuan untuk menahan laju virus di negara mereka*,* tak terkecuali di Indonesia. Di Indonesia, penerapan program serupa diwujudkan melalui Pembatasan Sosial Berskala Besar (PSBB). Situasi pandemi di Indonesia sendiri masih mengkhawatirkan. Jumlah terkonfirmasi positif mencapai 463.007 kasus pada 14 November 2020. Kondisi yang memaksa masyarakat untuk beraktivitas dari rumah telah mendorong percepatan transformasi teknologi digital, yang menyebabkan terjadinya disrupsi*.* Konsep inovasi disruptif menghasilkan kebaruan perilaku industri yang lebih efisien, yang kemudian menggantikan pasar lama (Christensen et.al 2018).

Pada kondisi disruptif, para pelaku industri berbondong-bondong mengadopsi teknologi informasi baru, sementara yang lain berpikir untuk mengganti model bisnis mereka, entah beralih ke layanan dan produk *online* atau menggunakan saluran bisnis baru (Caroell and Conboy 2020). Pola perilaku masyarakat yang sebelumnya masih menggunakan teknologi analog kemudian bermigrasi ke teknologi digital. Miliaran orang terhubung dengan perangkat seluler, kekuatan pemrosesan, kapasitas penyimpanan data, dan akses pengetahuan menjadi tak terbatas dengan teknologi baru seperti *Artificial Intelligence* (AI)*, Internet of Things* (IoT)*, nanotechnology,* dan *quantum computing* (Ozdemir and Hekim 2017). Transformasi digital mengarah kepada virtualisasi berkelanjutan dari proses bisnis inti. Proses virtual tersebut berlangsung di dalam maupun di luar perusahaan, yang mengarah ke lingkungan kolaboratif yang fleksibel. Sementara itu, Teknologi Informasi dan Komunikasi (TIK) membantu mewujudkan model bisnis ini. Teknologi digital yang sama akan sangat memengaruhi cara perusahaan berinovasi sambil menggunakan solusi cerdas untuk meningkatkan nilai pelanggan yang mengarah ke model bisnis dan penawaran layanan yang benar-benar baru (Ochs and Riemann 2017).

Transformasi digital di tengah pandemi menghadirkan era baru yang dikenal dengan istilah kenormalan baru*.* Yaitu, era ketika segala bentuk aktivitas, seperti transaksi keuangan beralih ke digital. Keadaan ini memberikan konsekuensi logis akan meningkatnya ancaman serangan siber yang dapat menyusup ke dalam setiap aktivitas sosial tersebut melalui TIK. International Business

Machines (IBM) memperlihatkan bahwa selama pandemi Covid-19, serangan siber global naik sebesar 6.000% (IBM 2020). Penjahat dunia maya terus mencari vektor serangan baru selama pandemi Covid-19. *Social distancing* yang dilakukan sebagai bentuk protokol kesehatan telah meningkatkan ketergantungan pada TIK, sehingga penjahat dunia maya dapat mengeksploitasi pandemi untuk memfasilitasi berbagai aktivitas kejahatannya, seperti mencoba mengambil alih platform konferensi video yang digunakan dalam rapat atau aktivitas pendidikan *online*, penipuan *online*, dan pencurian informasi data pribadi (S. Hakak et.al. 2020).

Meskipun jenis serangan siber tidak banyak berubah, Covid-19 telah memberikan peluang bagi para penjahat untuk dapat mengeksploitasi celah-celah baru. Situasi ini mampu meningkatkan intensitas serangan siber dan membuat keamanan data masyarakat menjadi makin terancam. Upaya menjaga privasi individu menjadi lebih rumit di tengah adanya kebutuhan untuk mendukung upaya kesehatan masyarakat selama pandemi yang memerlukan pengawasan global dengan bantuan teknologi digital baru (Radanliev et.al. 2020). Interpol menyebutkan bahwa lanskap kejahatan siber global selama pandemi Covid-19 didominasi oleh beberapa jenis serangan, yaitu (1) *scam* dan *online phising*, (2) *disruptive malware*, (3) *data harvesting malware,* (4) *malicious domain,* dan (4) *misinformation* (Interpol 2020). Jenis kejahatan siber dapat dibagi menjadi 2 (dua) kelompok. Pertama adalah kelompok *cyber dependent crime,* yaitu kejahatan yang hanya dapat dilakukan dalam *cyberspace* dengan menggunakan TIK, seperti praktik peretasan, pencurian data elektronik, penyerangan *Distributed Denial of Service* (DDOS) pada sistem server, dan distribusi *malware.* Kedua adalah kelompok *cyber enabled crime,* atau modus kejahatan tradisional yang telah ditingkatkan skala dan jangkauannya menggunakan TIK, contohnya seperti praktik penipuan *online* dan pencurian data pribadi melalui *phising* (McGuire and Dowling 2013).

Interpol pun menyebutkan bahwa serangan siber terjadi karena kesadaran masyarakat akan keamanan siber (*security awareness*) masih tergolong rendah, terutama di negara-negara di wilayah Asia dan Selatan Pasifik, termasuk Indonesia. Bank Indonesia menemukan bahwa tingkat kewaspadaan masyarakat Indonesia terhadap tindak kejahatan sektor *financial service,* khususnya pada Alat Pembayaran Menggunakan Kartu (APMK) dan Uang Elektronik (UE) hanya sebesar 36,32% (Bank Indonesia 2018). Survei Badan Siber dan Sandi Negara (BSSN) terhadap kerentanan di sektor keuangan dan perbankan menunjukkan bahwa minimnya *security awareness* adalah faktor terbesar yang menyebabkan terjadinya serangan siber. BSSN mencatat tingkat *awareness* mencapai 49% (Kurniawan 2020). Padahal, sekuat apa pun sistem yang melindungi keamanan data, faktor manusia tetaplah merupakan faktor dominan (50%) yang menjadi kunci keamanan informasi. BSSN juga mencatat peningkatan jumlah serangan selama pandemi yang mencapai 189.937 ribu kasus dibandingkan sebelum masa pandemi atau tahun 2019, yang hanya tercatat 39.330 kasus. Serangan siber di sektor keuangan melibatkan aktivitas *phising*, OTP (*One Time Password*) *fraud*, SIM SWAP, dan pembobolan data pribadi akun pengguna *e-commerce*. Selain menggunakan teknologi, penyerang juga menggunakan metode *social engineering* atau penipuan dengan teknik mempelajari dan memanipulasi psikis seseorang sehingga didapat data dan akses kemanan pribadi secara ilegal. *Open Source Intelligence (Osint)* atau teknik pengumpulan bahan keterangan melalui sumber-sumber terbuka seperti dari media sosial adalah pendekatan yang sering digunakan.

Data pribadi adalah semua data yang berhubungan dengan orang per orang yang teridentifikasi (Freeman and Van Ert 2004). Kebijakan perlindungan data pribadi sebagai hak privasi semua orang harus bersifat dinamis dan antisipatif karena sangat dipengaruhi perkembangan lingkungan, seperti kemajuan TIK maupun perkembangan inovasi bisnis. Dalam

memberikan perlindungan keamanan data bagi warganya, beberapa negara telah membangun *framework policy* melalui proses yang dibangun dari bawah ke atas *(bottom up)*, yaitu dengan mengikuti perkembangan TIK sebagai bentuk formalisasi dari dinamika transformasi digital yang terus berubah di masyarakat. Sebuah negara dapat mencapai ketahanan sibernya jika telah memiliki strategi dan kebijakan di bidang keamanan siber (Rahmawati 2017). Tujuan umum keamanan siber adalah untuk melindungi jaringan TIK dan sistem informasi dari segala potensi ancaman. Suatu sistem dapat dikatakan tangguh apabila dapat menyelamatkan kepentingan yang lebih luas di dalamnya, bahkan ketika menghadapi peristiwa siber yang merugikan sekalipun (Björck et.al. 2015). Salah satu upaya untuk menjaga kepentingan tersebut adalah dengan melakukan perlindungan data pribadi, yang merupakan bagian dari hak asasi manusia yang perlu dijamin oleh pemerintah bagi warga negaranya, terlebih di era kenormalan baru saat ini. Warren (1890) meletakkan prinsip dasar hak privasi sebagai hak asasi untuk menikmati hidup dan menuntut hukum untuk melindungi hak privasi.

Interpol (2020) memperlihatkan adanya kerentanan serangan siber di wilayah Eropa dan Asia selama pandemi Covid-19 tetapi belum menjelaskan secara spesifik perbandingan strategi kebijakan di masing-masing wilayah. Hal ini dilengkapi oleh penelitian sebelumnya (Sunkpho et.al. 2018) yang menjelaskan bahwa dibandingkan 5 (lima) negara ASEAN lainnya (Malaysia, Singapura, Thailand, Vietnam dan Filipina), hanya Indonesia yang tidak memiliki undang-undang keamanan siber dan undang-undang kejahatan siber secara khusus. Indonesia hanya memiliki Undang-Undang Informasi dan Transaksi Elektronik yang dipaksakan untuk mengakomodasi kompleksitas urusan keamanan siber nasional. Terkait masalah keamanan data, hanya Thailand dan Indonesia yang belum memiliki undang-undang perlindungan data pribadi. Bahkan, negara komunis seperti Vietnam telah memiliki hukum komprehensif yang mengatur keamanan dan perlindungan data dalam satu regulasi bernama *Law Cyber Information Security* (LCIS).

Di Indonesia, Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi yang diniatkan sebagai upaya perlindungan, masih berada dalam proses pembahasan Daftar Inventaris Masalah (DIM) antara pemerintah dengan Dewan Perwakilan Rakyat Republik Indonesia (DPR RI). Sayangnya, situasi ancaman serangan siber terhadap keamanan data pribadi selama pandemi tidak bisa menunggu lebih lama lagi. Regulasi eksisting yang memproteksi ancaman serangan siber terhadap keamanan data masih berdiri sendiri-sendiri. Dewi Rosadi (2015) menemukan bahwa masalah data pribadi sebagai hak privasi di berbagai bidang dapat ditemukan di beberapa peraturan perundang-undangan serta peraturan teknis yang terpisah.

Penelitian ini melakukan *benchmarking* situasi serangan siber dan regulasi perlindungan data pribadi di Indonesia dengan negara yang memiliki penanganan kejahatan siber yang lebih baik. Metodenya adalah dengan membandingkan elemen naratif berupa *hero, villain,* dan *victim* yang ada pada masing-masing negara, menggunakan metode analisis Narrative Policy Framework (NPF). NPF mampu mengkaji sebuah kebijakan secara *peer to peer* melalui elemen naratif dengan mengupas kelemahan fundamental kebijakan Indonesia dibandingkan dengan negara lainnya dalam menangani serangan siber selama pandemi Covid-19, sehingga dapat menjadi landasan membangun solusi kebijakan yang tepat sasaran. Kemunculan NPF sebagai bagian dari paradigma riset tidak lepas dari paradigma *structuralism* dan *post-structuralism*, yang berkontribusi pada kemunculan dan perkembangan NPF sebagai pendekatan riset, baik riset *positivistic* maupun riset *post-positivistic* (Salahudin 2019). Tradisi riset NPF sangat membantu untuk menggambarkan fenomena sosial yang berhubungan dengan narasi dan strategi aktif dan *social groups* dalam proses kebijakan publik *(ibid)*.

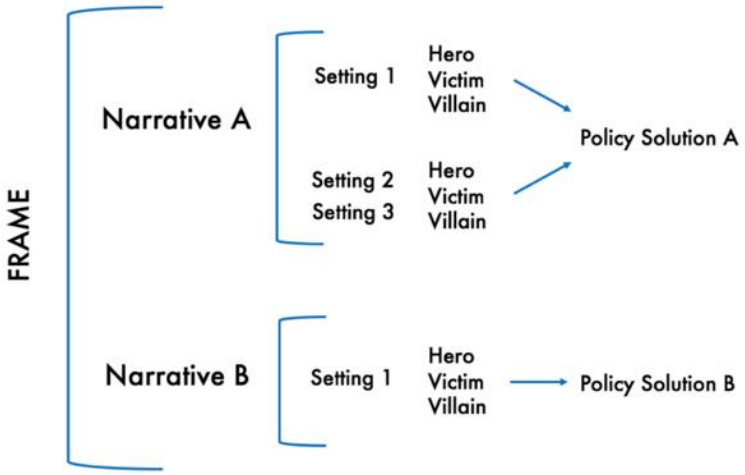
eISSN 2527 - 4902

Benchmarking merupakan teknik membandingkan dan mengukur jalannya sebuah organisasi atau cara membandingkan dan mengukur internal organisasi secara berulang-ulang dengan organisasi yang mempunyai kelas lebih tinggi, baik dari dalam atau dari luar organisasi perusahaan (Goestsch and Davis 1997). Dalam hal ini, perbandingan organisasi yang dimaksud dalam *scope* yang lebih besar adalah *benchmarking* yang dilakukan antarnegara. Negara-negara yang dipilih dalam studi *benchmarking* ini adalah Indonesia, Inggris Raya, dan Malaysia. Inggris Raya merupakan bagian dari negara-negara Eropa yang memelopori prinsip-prinsip dasar regulasi perlindungan data pribadi di dunia. Malaysia telah lama menerapkan regulasi perlindungan data pribadi bagi warganya dengan mengadopsi norma perlindungan data pribadi dari Uni Eropa. Malaysia pun memiliki kedekatan geografis dengan Indonesia. Dengan membedah regulasi perlindungan data pribadi di ketiga negara tersebut, diharapkan akan ditemukan pesan moral dan sistem keyakinan terhadap regulasi perlindungan data pribadi yang dapat diterapkan di Indonesia.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis Narrative Policy Framework (NPF). NPF mampu menjelaskan proses dan narasi kebijakan secara empiris mengenai berbagai masalah kebijakan pada level analisis tertentu (Jones and Shanahan 2014). NPF dinilai sebagai pendekatan riset yang tepat untuk digunakan dalam konteks riset *post-positivistic*, karena itu akhir-akhir ini banyak peneliti tertarik menggunakan pendekatan NPF dalam riset-riset mereka, khususnya riset yang berkaitan dengan isu *big data, social media*, narasi kebijakan, strategi politik, dan perilaku sosial budaya dalam konteks kebijakan publik (Salahudin 2019). Penelitian ini menggunakan level analisis tingkat *meso* dengan melakukan studi *benchmarking* antara Indonesia dengan negara-negara pembanding, yaitu Inggris Raya dan Malaysia.

Bentuk telaah masing-masing kebijakan melalui metodologi analisis NPF secara sederhana dapat dilihat lebih jelas pada Gambar 1.



Gambar 1. Bagan Narrative Policy Framework (French et.al. 2017)

Pada masing-masing negara, akan dilakukan *benchmarking* mengenai kerangka kebijakan melalui beberapa elemen naratif, yaitu: *setting* dan karakter yang meliputi *hero, victim,* dan *villain*. *Heroes* adalah pihak yang mampu memecahkan masalah, *villains* adalah pihak yang menyebabkan masalah, dan *victims* adalah pihak yang dirugikan. Karakter dalam NPF tidak harus manusia, tetapi dapat berupa objek abstrak. Dari karakter tersebut disusun plot naratif kebijakan dengan menghubungkan masing-masing karakter dalam pengaturan kebijakan secara lengkap.

Kebijakan yang diterapkan oleh setiap negara tersebut ditelaah dengan mengamati kasus serangan siber yang terjadi di tiap negara selama berlangsungnya pandemi Covid-19, sehingga ditemukan kesenjangan antara keadaan di Indonesia dan negara pembanding. Temuan kesenjangan ini selanjutnya digunakan untuk menemukan solusi kebijakan yang perlu dilakukan Indonesia dalam memperkuat perlindungan keamanan data pribadi di Indonesia, khususnya di masa kenormalan baru.

HASIL DAN PEMBAHASAN

Regulasi Perlindungan Data Pribadi di Ketiga Negara

1) Inggris Raya

Kebijakan perlindungan keamanan data pribadi di Inggris Raya dan negara-negara Eropa lainnya memiliki sejarah yang sangat panjang. Pertama kalinya hak privasi diatur dalam Deklarasi Universal Hak Asasi Manusia adalah setelah Perang Dunia II. Menimbang arti penting dari perlindungan hak privasi, pada tahun 1970 Jerman menetapkan kebijakan perlindungan data pribadi melalui Undang-Undang Perlindungan Data. Langkah ini diikuti oleh Inggris dan negara-negara Eropa lainnya seperti Swiss, Austria, Swedia, dan Perancis. Di tahun 1980, negara-negara Eropa yang tergabung dalam Organization for Economic Co-Operation and Development (OECD) mengeluarkan *Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data.* Pedoman tersebut diadopsi menjadi prinsip normatif internasional terkait pengelolaan data privasi yang meliputi pembatasan pengumpulan, kualitas data, spesifikasi tujuan, pembatasan pengungkapan data, langkah pengamanan, keterbukaan, partisipasi individu, dan pertanggungjawaban. Di tahun 1981 dibentuklah the Council of Europe Convention yang memaksa negara-negara Eropa untuk berkomitmen dalam memegang teguh prinsip-prinsip yang menjamin hak dasar individu terhadap *data privacy* di wilayah mereka, yang diatur berdasarkan peraturan perundang-undangan yang berlaku di negara masing-masing.

Kasus Snowden di tahun 2013 memantik respons berbagai pihak dan mendorong lahirnya Resolusi PBB 68/167 tentang the Right to Privacy in the Digital Age di tahun 2013. Resolusi ini membuka kesadaran banyak pihak akan ancaman berupa pengawasan secara diam-diam dan intersepsi komunikasi yang dilakukan secara ilegal, termasuk kerentanan pengumpulan data pribadi secara ilegal melalui serangan siber. Sementara itu, pada Kovenan Internasional Hak-Hak Sipil dan Politik, dijelaskan bahwa pengumpulan dan penyimpanan informasi pribadi melalui berbagai piranti elektronik oleh siapa pun harus diatur dengan jelas secara hukum. Tujuannya untuk memastikan bahwa informasi data pribadi seseorang tidak sampai ke pihak yang tidak bertanggung jawab. Undang-Undang Perlindungan Data Pribadi terus berkembang dan mencapai puncaknya di tahun 2016 ketika terjadi simplifikasi terhadap semua proses yang terkait dengan data pribadi di Uni Eropa menjadi satu regulasi dalam European Union-General Data Protection Regulation (EU-GDPR). Regulasi ini mulai aktif digunakan pada bulan Mei 2018 dan telah diadopsi oleh lebih dari 125 negara di dunia sebagai acuan undang-undang perlindungan data di negaranya (Wahyudi and M. Jodi 2019).

Berdasarkan EU-GDPR tersebut, seseorang memiliki hak untuk mengetahui informasi apa yang disimpan pemerintah dan organisasi lain tentang dirinya, termasuk hak untuk diberitahu tentang bagaimana data yang bersangkutan digunakan, akses data pribadi, memperbaharui data yang salah, menghentikan atau membatasi proses data yang bersangkutan, mendapatkan dan menggunakan kembali *file* data yang digunakan, dan menolak proses data. Undang-Undang

Perlindungan Data mewajibkan pemrosesan data pribadi yang adil, yang menuntut pemerintah atau organisasi lain untuk transparan tentang latar belakang pengumpulan data pribadi dan cara menggunakannya. Undang-Undang ini bahkan mengatur kewajiban organisasi untuk mendapatkan persetujuan dari pengguna situs web saat menempatkan *cookies* atau teknologi serupa di komputer dan perangkat seluler mereka. Ada tujuh prinsip perlindungan data pada Undang-Undang ini, yaitu: (1) digunakan secara adil sesuai hukum dan diproses secara transparan, (2) digunakan untuk tujuan tertentu dan eksplisit, (3) digunakan dengan cara yang memadai, relevan dan terbatas hanya pada apa adanya, (4) akurat dan jika perlu selalu diperbarui, (5) data pribadi harus disimpan dalam bentuk yang memungkinkan identifikasi subjek data tidak lebih dari yang diperlukan (batasan penyimpanan), (6) data pribadi harus diperlakukan dengan memastikan keamanan data pribadi yang sesuai, dan (7) akuntabilitas.

Meskipun regulasi dan perangkat perlindungan hukum terkait data pribadi di Inggris Raya terbilang sangat matang, nyatanya hal tersebut belum dapat menekan potensi ancaman keamanan data di negara mereka. Selama pandemi Covid-19, insiden serangan siber di Inggris Raya mengalami peningkatan. Lanskap serangan siber di Inggris Raya menyasar pada serangan *critical infrastructure* dan penipuan *online* melalui *phising* pada sektor kesehatan. The National Cyber Security Center (NCSC) di Inggris Raya telah melaporkan bahwa penjahat dunia maya sering kali menyamar sebagai institusi resmi kesehatan, seperti sebagai Pusat Pengendalian Penyakit. Mereka membuat nama domain seperti alamat web yang menyerupai instansi tersebut kemudian meminta kata sandi dan melancarkan modus untuk meminta data pribadi dan sumbangan *bitcoin* untuk mendanai vaksin palsu (UNODC 2020). Negara-negara Uni Eropa seperti Inggris Raya memiliki suatu organisasi independen nonprofit bernama Information Sharing and Analysis Centers (ISACs). Organisasi ini menyediakan sumber daya sentral untuk mengumpulkan informasi tentang ancaman dunia maya (terutama pada infrastruktur kritis) dan bertindak sebagai penghubung yang memungkinkan terjadinya *sharing* informasi dua arah antara sektor swasta dan pemerintah dalam mencari akar penyebab, insiden dan ancaman, serta berbagi pengalaman, pengetahuan, dan analisis di berbagai sektor.

Peningkatan insiden kejahatan siber di Inggris Raya selama pandemi Covid-19 ditandai dengan bertambahnya jumlah *email* laporan pengaduan penipuan *online* yang terjadi di negara tersebut. Pada awal Mei, lebih dari 160.000 email 'tersangka' telah dilaporkan ke NCSC dan pada akhir Mei 2020 terjadi kerugian sebesar £4,6 juta karena penipuan terkait Covid-19 yang melibatkan sekitar 11.206 korban penipuan *online* pencurian data pribadi bermodus *phising* (H. Lallie, L. Shepherd, J. Nurse et.al. 2020). Merespons laporan tersebut, NCSC segera menghapus 471 *e-commerce* palsu dan HMRC (Her Majesty's Revenue and Customs) juga menghapus 292 situs palsu *(ibid)*. Untuk mengantisipasi maraknya serangan siber, Pemerintah Inggris Raya meningkatkan literasi untuk membangun kesadaran warganya terhadap maraknya penipuan *online* menggunakan *phising.* Pada tanggal 8 April 2020, NCSC bekerja sama dengan Department of Homeland Security Cyber, Cyber Security and Infrastructure Security Agency (CISA) dari Amerika Serikat untuk segera mengeluarkan kebijakan tentang informasi bentuk kejahatan siber dan serangan siber tingkat lanjut serta cara pencegahannya selama pandemi Covid-19 melalui pengumuman dan sosialisasi *(ibid)*.

2) Malaysia

Pembahasan regulasi perlindungan data pribadi di Malaysia secara khusus sudah ada sejak tahun 1998. Baru di tahun 2010 disahkanlah Personal Data Protection Act (PDPA) sekaligus dibentuk Departemen Perlindungan Data di bawah naungan Kementerian Informasi Komunikasi dan Kebudayaan untuk menangani implementasi PDPA (Greenleaf 2014). Ada 7 (tujuh) prinsip

yang diatur dalam PDPA, yaitu: (1) prinsip umum pengolahan data berdasarkan persetujuan, (2) prinsip pengumpulan dan pemberitahuan, (3) prinsip penggunaan dan pengungkapan, (4) prinsip keamanan, (5) prinsip retensi dan hak untuk memblokir pemrosesan, (6) prinsip integritas data, (7) prinsip akses dan koreksi (Dewi Rosadi 2015). Selain Undang-Undang PDPA yang mengatur keamanan atas hak privasi warga negaranya, ada pula Undang-Undang KUHP di Malaysia yang mengatur sanksi dan denda terkait data privasi.

Di tahun 2017, Pemerintah Malaysia kemudian mendirikan badan keamanan siber nasional bernama National Cyber Security Agency (NCSA). Badan ini bertugas untuk mengamankan dan memperkuat ketahanan siber negara Malaysia, termasuk ancaman serangan siber terhadap keamanan data pribadi. Lingkup kerja NCSA adalah menerapkan kebijakan keamanan siber serta melindungi *critical infrastructure* nasional. Menurut laporan dari NCSA, selama pandemi Covid-19, terjadi peningkatan aktivitas penipuan dan *malware* yang menggunakan tema Covid-19 untuk menipu korban sehingga korban mau memberikan informasi pribadi dan memasang aplikasi *malware.* Selain NCSA, Malaysia juga memiliki *command center* bernama National Cyber Coordination and Command Centre (NC4). NC4 adalah gugus tugas yang terdiri dari NCSA dan sejumlah unsur yang menangani ketahanan siber di berbagai sektor seperti di pemerintahan, perbankan, dan pertahanan.

Serangan siber di Malaysia selama pandemi memanfaatkan masalah kesehatan masyarakat dan Covid-19. Penyerang akan menarik korban masuk ke dalam perangkap mereka. Kelompok besar yang mendapat perhatian di Malaysia adalah Advanced Persistent Threat (APT) Group. Kelompok ini dicurigai mendapatkan dukungan dari "*actor state"* dan melakukan kombinasi *cyber espionage* dan *cybercrime* (FireEye 2020). Mereka menyerang negara-negara maju dan biasanya melancarkan serangan dengan modus mencuri data, mengganggu operasi, atau menghancurkan infrastruktur. Tidak seperti kebanyakan penjahat dunia maya, penyerangan APT Group mengejar tujuan mereka selama berbulan-bulan atau bertahun-tahun. Mereka beradaptasi dengan pertahanan dunia maya yang kuat dan sering mengincar korban yang sama. Serangan siber dari kelompok semacam ini bervariasi, mulai dari *business email compromise*, *malware, ransomware,* dan penipuan telepon. Semua diatur oleh kelompok APT Group dan kelompok kejahatan terorganisasi lainnya dengan memanfaatkan situasi ini untuk serangan terbaru mereka.

Untuk menghadapi serangan siber yang kian meningkat semasa pandemi Covid-19, Perdana Menteri Malaysia meminta NC4, NACSA, dan NSC untuk mengooordinasikan publikasi yang bertujuan mengingatkan semua warganya agar waspada dan terus menjaga praktik higienitas dunia maya saat bekerja dari rumah. Pengumuman dan sosialisasi ini berisi pedoman *work from home* dengan aman, seperti: (1) selalu memverifikasi informasi apa pun yang diterima dari *email*, pesan teks, dan unggahan media sosial tentang Covid-19 (2) menggunakan koneksi *Virtual Private Network* (VPN) untuk mengakses sumber daya internal, (3) tidak membuka tautan atau *email* yang mencurigakan, (4) tidak mengunjungi situs web yang tidak terpercaya, (5) tidak memberikan informasi pribadi seperti alamat *email* atau *password*, (6) mengubah *password* jika merasa aksesnya dicuri, dan (7) terus memperbarui ponsel dan sistem operasi serta aplikasi komputer secara teratur, dan himbauan lainnya yang dinilai berguna untuk menghindari serangan siber selama *work from home* (NACSA 2020).

3) Indonesia

Di tengah situasi pandemi Covid-19, Indonesia belum memiliki regulasi khusus tentang keamanan data pribadi di dunia maya. Kebijakan tentang keamanan data pribadi hanya terdapat dalam Pasal 26 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan

revisinya di tahun 2016 yang mengatur bahwa penggunaan data pribadi harus dilakukan dengan persetujuan orang yang bersangkutan dan bahwa setiap orang yang dilanggar haknya dapat mengajukan gugatan. RUU Perlindungan Data Pribadi yang menjadi program legislatif nasional tahun 2020 ini banyak mengadopsi prinsip-prinsip hak privasi perlindungan data yang berasal dari Uni Eropa. Belum adanya Undang-Undang tersebut membuat masalah keamanan data pribadi masih diproteksi melalui berbagai perundang-undangan yang berdiri secara terpisah seperti Undang-Undang Perbankan, Undang-Undang Telekomunikasi, Undang-Undang Perlindungan Konsumen, Undang-Undang Kependudukan, Undang-Undang Hak Asasi Manusia, Undang-Undang Administrasi Kependudukan, Undang-Undang Informasi Transaksi Elektronik (ITE), Undang-Undang Keterbukaan Informasi Publik, dan Undang-Undang Kesehatan. Selain itu, terdapat pula peraturan pendukung seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi.

Delik pidana terkait perlindungan data pribadi dapat dilihat di UU ITE pasal 30 ayat (2) yang berbunyi bahwa setiap orang, dengan sengaja dan tanpa hak atau melawan hukum, mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, maka di pasal 48 ayat (2) dapat dipidana dengan pidana paling lama penjara 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000. Selain itu, delik pidana juga ditemukan pada UU KUHP pasal 362 tentang pencurian biasa dan pasal 363 tentang pencurian dengan pemberatan. Delik pidana terkait data pribadi kependudukan juga ditemukan pada UU Kependudukan Nomor 24 Tahun 2013, di pasal 94, pasal 95a, pasal 96, dan pasal 96a. Peraturan perundang-undangan dan peraturan teknis yang membahas mengenai data pribadi hingga saat ini masih terpisah-pisah dan saling tumpang tindih satu sama lain. Indonesia memerlukan aturan khusus yang lebih sederhana yang dapat mengakomodasi segala aturan perlindungan data pribadi dari berbagai sektor. Hal tersebut diupayakan dalam RUU Perlindungan Data Pribadi.

Untuk menangkal peningkatan serangan siber di Indonesia, pemerintah mengeluarkan Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN). BSSN berasal dari gabungan dua institusi, yaitu Lembaga Sandi Negara dan Direktorat Jenderal Aplikasi Informatika (Aptika) Kementerian Kominfo. BSSN mempunyai tugas untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber di beberapa organisasi.

Sebagai langkah tindak lanjut penanganan serangan siber akibat rendahnya *security awareness* masyarakat di masa pandemi, Kementerian Kominfo, BSSN, Polri, Bank Indonesia (BI), Otoritas Jasa Keuangan (OJK) dan berbagai unsur berkolaborasi untuk meningkatkan literasi dan sosialisasi kepada masyarakat. Kegiatan ini berbentuk *webinar* serta publikasi iklan layanan masyarakat di berbagai media untuk memberikan pemahaman masyarakat mengenai beberapa jenis bentuk serangan siber yang sering muncul selama pandemi Covid-19 dan cara mengatasinya. Selain literasi ke masyarakat, BSSN juga berupaya memberikan layanan pendampingan dan fasilitasi kepada berbagai perusahaan di semua sektor untuk menerapkan standar keamanan siber dengan melakukan proteksi secara mandiri berdasarkan standar nasional (Indeks Keamanan Informasi, KAMI) maupun standar internasional (ISO 27001).

Hasil *Benchmarking* melalui Narrative Policy Framework

Dari pembahasan kebijakan perlindungan data pribadi dan serangan siber selama pandemi Covid-19 yang terjadi di Inggris Raya, Malaysia, dan Indonesia, maka dapat disusun identifikasi elemen naratif pada ketiga negara berdasarkan karakternya seperti tampak pada Tabel 1.

Tabel 1. Identifikasi Elemen Naratif Karakter berdasarkan NPF Analysis

No	Karakter	Inggris Raya	Malaysia	Indonesia
1.	*Hero*	- Regulasi: EU-GDPR - Organisasi: NCSC, NC4, ISACs - Literasi: peningkatan *security awareness*	- Regulasi: PDPA - Organisasi: NACSA - Literasi: peningkatan *security awareness*	- Regulasi: KUHP, UU ITE, UU Perbankan, UU Telekomunikasi, UU Perlindungan Konsumen, UU Kependudukan, UU Hak Asasi Manusia, UU Administrasi Kependudukan, Undang-Undang Keterbukaan Informasi Publik, UU Kesehatan, PP No 71/2019, Permen Kominfo No 20/2016 - Organisasi: BSSN - Literasi: peningkatan *security awareness*
2.	*Villain*	- Serangan siber - *Security awareness*	- Serangan siber - *Security awareness*	- Serangan siber - *Security awareness* - Belum adanya regulasi terpadu untuk perlindungan data pribadi
3.	*Victim*	- Keamanan data pribadi warga - Keamanan data pribadi dari pelaku industri	- Keamanan data pribadi warga - Keamanan data pribadi dari pelaku industri	- Keamanan data pribadi warga - Keamanan data pribadi dari pelaku industri

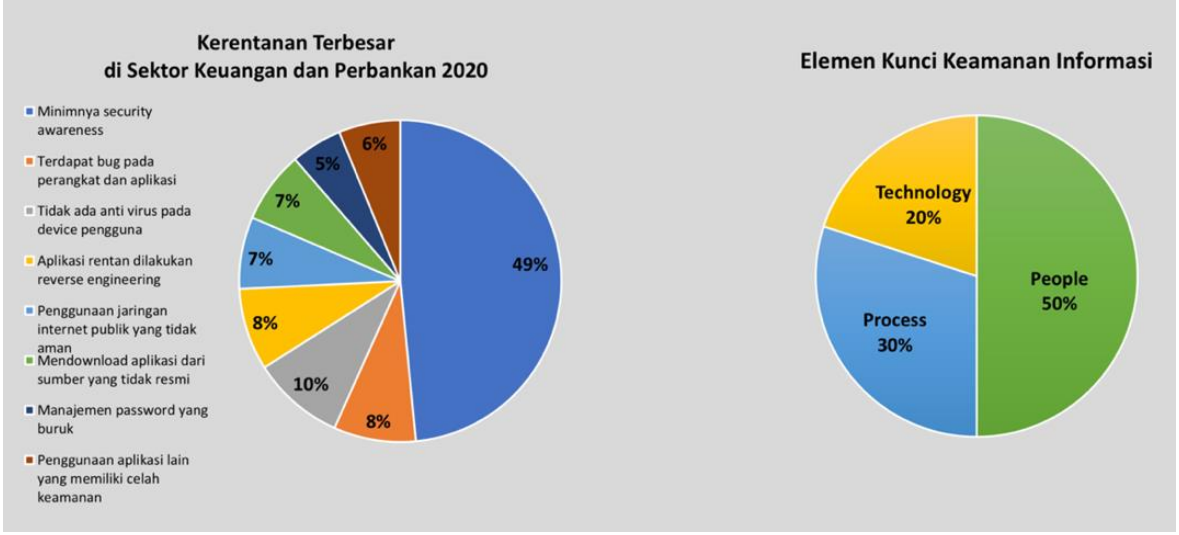
Sumber: Hasil olah data penelitian

Setting kebijakan perlindungan data pribadi di Inggris Raya dan Malaysia telah terakomodasi di dalam satu produk perundang-undangan perlindungan data pribadi yang terintegrasi. Ketiga negara telah memiliki *hero* dalam kebijakan dan lembaga penanganan serangan siber. Untuk kebijakan, Inggris Raya memiliki EU-GDPR dan Malaysia memiliki PDPA. Namun, di Indonesia, kebijakan perlindungan data pribadi sementara ini masih terpisah-pisah dan belum terintegrasi. Saat ini, untuk menjerat serangan siber, pihak berwenang menggunakan UU ITE dan peraturan lainnya yang relevan dengan tindak ilegal. Kehadiran *hero* juga didukung dengan adanya badan khusus yang menangani serangan siber. Inggris Raya memiliki NCSC, Malaysia memiliki NACSA, dan Indonesia memiliki BSSN. Untuk mensinergikan pengelolaan sistem TIK penting lintassektor, pemerintah Malaysia membentuk Pusat Koordinasi dan *Command Center* yang mengelola manajemen krisis siber nasional di berbagai sektor. *Command Center* ini bernama National Cyber Coordination and Command Centre (NC4). NC4 merupakan solusi Pemerintah Malaysia untuk membangun koordinasi lintassektor dalam penanggulangan serangan siber agar dapat menjadi lebih efektif. Di Inggris Raya, model kerja sama dan koordinasi antara pihak swasta dan pemerintah tersebut diperkuat dengan dibentuknya organisasi nonprofit bernama ISACs. Indonesia sendiri masih belum memiliki model kerja sama lintassektor seperti yang dilakukan oleh Malaysia dan Inggris Raya. Karakter *hero* tidak hanya terlihat pada kebijakan

eISSN 2527 - 4902

dan lembaga penanganan serangan siber tetapi juga pada peningkatan literasi masyarakat. Ketiga negara menyadari rendahnya *security awareness* sehingga perlu ditingkatkan melalui literasi dan sosialisasi, baik kepada masyarakat maupun pelaku industri, mengenai bentuk serangan siber selama pandemi dan tindak pencegahannya.

Karakter *villain* dalam *setting* kebijakan perlindungan data pribadi ditunjukkan oleh serangan siber dan rendahnya *security awareness* di masyarakat. Meskipun telah memiliki regulasi perlindungan data pribadi, serangan siber di Inggris Raya dan Malaysia tidak serta merta terkendali. Regulasi yang tersedia belum mampu menekan intensitas serangan siber selama pandemi Covid-19. Regulasi tersebut hanya memberikan kepastian hukum dalam pengelolaan data pribadi dan perlindungannya dari ancaman siber, sekaligus mengatur sanksi dan denda apabila ada perlakuan ilegal terhadapnya. Rendahnya *security awareness* di masyarakat sebagai dampak dari peningkatan aktivitas secara *online* dan paksaan untuk mengadopsi teknologi semakin memperparah keadaan. Minimnya *security awareness* di Indonesia diperlihatkan oleh hasil survei yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), seperti tampak pada Gambar 2.



Gambar 2. Kerentanan di Sektor Keuangan dan Perbankan, serta Elemen Kunci Keamanan Informasi (Kurniawan 2020)

Dari Gambar 2 didapatkan informasi bahwa faktor kerentanan terbesar di sektor keuangan dan perbankan adalah karena minimnya *security awareness,* yaitu sebesar 49%. Adapun faktor manusia tetaplah merupakan faktor dominan (50%) yang menjadi kunci keamanan informasi. Dengan demikian, sangat penting bagi para pemangku kebijakan untuk memberikan literasi secara masif dan terstruktur ke seluruh lapisan masyarakat dengan menggunakan semua lini media guna meningkatkan pengetahuan terhadap keamanan data pribadi di Indonesia selama pandemi Covid-19. Hakak *et al*. (2020) menjelaskan bahwa literasi keamanan siber pada masa pandemi Covid-19 harus mencakup beberapa hal, yaitu: panduan keamanan yang membantu masyarakat untuk dapat mengamankan perangkat mereka masing-masing, *Virtual Private Network* (VPN) yang harus digunakan saat bekerja dari rumah sebagai sarana komunikasi antara perangkat pribadi karyawan dan sistem perusahaan, dan kesadaran *cybersecurity* yang harus ditingkatkan secara berkala melalui program pendidikan dan pelatihan tentang *cybersecurity.*

Di Indonesia, kondisi semakin memburuk dengan belum adanya regulasi terpadu untuk perlindungan data pribadi, yang merupakan representasi dari karakter *villain* tambahan yang harus dihadapi bangsa ini. Adapun dari sisi *victim*, korban utama dari serangan siber di ketiga

negara adalah keamanan data pribadi warga. Masyarakat menempati posisi lemah dari tindakan para penyerang ini sehingga penjahat bisa memanfaatkannya untuk mengeksploitasi hadirnya kejahatan lainnya seperti menguras rekening korban. Kondisi ini memerlukan perlindungan atas hak-hak privasi masyarakat. Selain masyarakat, pelaku industri juga rentan terhadap serangan siber. Terdapat kerentanan yang menonjol di lapangan, yaitu rendahnya kesadaran terhadap keamanan data pribadi *(security awareness)* akan bahaya serangan siber. Hal ini merupakan ancaman terbesar keamanan data pribadi dari serangan siber, khususnya di era kenormalan baru. Jika melihat urgensi akan perlunya meningkatkan *security awareness* masyarakat di segala lapisan, maka ada kebutuhan untuk memasukkan kurikulum keamanan siber tingkat dasar di sekolah dan pendidikan tinggi, terutama di era kenormalan baru. Sejauh ini, strategi komunikasi yang telah dilakukan pemerintah untuk memberikan literasi kepada masyarakat melalui *webinar* dan konten infografis masih terbatas kasus per kasus. Jadi, ke depan memang perlu ditanamkan pemahaman yang lebih komprehensif terkait pedoman praktis untuk menjaga keamanan data pribadi dari serangan siber secara umum, seperti yang juga dilakukan oleh Malaysia dan Inggris Raya selama pandemi Covid-19.

Dengan mengidentifikasi karakter *hero, villain,* dan *victim* tersebut, terlihat aspek kelemahan mendasar dan implikasi yang muncul dari penanganan serangan siber di Indonesia, yaitu belum tersedianya *framework* kebijakan dan regulasi yang dapat menangani kompleksitas serangan siber dan keamanan data secara komprehensif di Indonesia. Kondisi eksisting yang terjadi adalah penanganan yang masih terpisah-pisah pada masing-masing sektor. UU ITE masih mencampur masalah hukum keamanan siber dan hukum kejahatan siber ke dalam satu aturan sehingga terjadi hambatan dalam penanganan kasus serangan siber yang kompleks. Menurut Ramli (2020), model *framework* regulasi terhadap masalah serangan siber yang ideal di dunia dapat dibagi ke dalam 3 (tiga) kelompok berdasarkan penanganannya, yaitu hukum keamanan siber, kejahatan siber dan perlindungan data, sebagaimana terlihat pada Tabel 2.

Tabel 2. Identifikasi *Framework* Regulasi terhadap Serangan Siber (Ramli 2020)

Hukum Keamanan Siber	Hukum Kejahatan Siber	Hukum Perlindungan Data
- Perlindungan infrastruktur - Memungkinkan sektor untuk bekerja sama, berkoordinasi, berbagi informasi, *intelligence sharing* - Orientasinya adalah menghentikan serangan siber, bukan menangkap aktor kejahatan	- Aktivitas kriminal - Berfokus pada aktor kejahatan - Mendefinisikan tindakan kriminal - Kerja sama internasional dan bantuan antara penegak hukum	- Data pribadi - Penanganan data sensitif, tata kelola dan perlindungan yang diberikan - Berlaku untuk semua pihak dan sektor yang mengelola data pribadi, baik pada aktivitas *online* maupun *offline*

Sumber: Hasil olah data penelitian

Dari berbagai implikasi yang teridentifikasi melalui analisis NPF tersebut, maka solusi kebijakan yang perlu segera dilakukan Pemerintah Indonesia untuk mengatasi serangan siber selama era kenormalan baru di masa pandemi Covid-19 yaitu:

1) Percepatan pengesahan RUU Perlindungan Data Pribadi

Indonesia memiliki ketertinggalan soal ketersediaan perlindungan hukum data pribadi secara lebih komprehensif di semua sektor. Ardiyanti (2014) menjelaskan bahwa kepastian hukum dalam pembangunan *cyber security* terkait dengan ketersediaan dokumen *security policy* yang dapat dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi. Untuk itu, pembahasan RUU Perlindungan Data Pribadi yang telah dilakukan saat ini perlu dipercepat

dengan tetap mengedepankan prinsip kehati-hatian dan antisipatif terhadap perkembangan TIK yang begitu cepat. Hukum mengenai perlindungan data pribadi inilah yang akan menangani berbagai masalah data sensitif dan tata kelola serta perlindungan data, baik dalam aktivitas *online* maupun *offline*. Prinsip perlindungan data pribadi secara umum mengatur beberapa aspek penting, seperti kedudukan data pribadi berdasarkan persetujuan, relevansi dengan tujuan, kemudahan akses, keutuhan, akurasi, dan keabsahan serta kemutakhiran data pribadi. Proses pembahasan RUU Perlindungan Data Pribadi antara pemerintah dan DPR RI perlu mempertimbangkan agar aturan tersebut nantinya mampu mengintegrasikan seluruh peraturan eksisting yang sebelumnya terpisah-pisah, mencakup seluruh jenis data pribadi, hak pemilik data, pemrosesan data, pengecualian, kewajiban dan tanggung jawab pengendali data, transfer data, penyelesaian sengketa, hingga ketentuan sanksi, baik administrasi maupun pidana.

2) Tersedianya regulasi khusus yang menangani keamanan siber dan kejahatan kriminal siber

Kompleksitas ancaman serangan siber di sektor publik, pemerintahan dan sektor swasta, memerlukan penanganan berupa tersedianya 2 (dua) produk regulasi yang secara khusus mengatur tentang keamanan siber dan kejahatan siber, baik yang berasal dari kejahatan domestik maupun transnasional. Hukum keamanan siber harus menaungi masalah perlindungan infrastruktur kritis dari serangan siber dan koordinasi lintassektoral yang seharusnya diatur dalam suatu regulasi tentang *cybersecurity*. Indonesia juga seharusnya memiliki wadah organisasi independen yang mampu menjalin kerja sama lintassektoral dalam penanganan kasus-kasus siber, baik itu di pemerintahan, swasta, maupun sektor publik. Kejahatan siber seharusnya terakomodasi dalam regulasi yang khusus mengatur masalah aktivitas kejahatan kriminal siber, berbagai bentuk aktivitasnya, serta penanganannya baik secara nasional maupun transnasional bersama dengan penegak hukum di negara lain.

3) Pembangunan ekosistem penanganan keamanan siber lintassektor

Ancaman serangan siber di era kenormalan baru makin kompleks dan meluas di berbagai sektor, sehingga sangat diperlukan koordinasi dan sinergi yang optimal antara BSSN dengan unsur-unsur penanganan siber yang ada di berbagai organisasi, seperti *Cyber Crime* Polri, Kementerian Kominfo, Badan Intelijen Negara (BIN) dan unsur keamanan siber di berbagai sektor industri. Ego sektoral yang masih terjadi selama ini membuat penanganan siber di Indonesia menjadi tersendat-sendat, sehingga kasus penipuan *online* dan pembobolan data pribadi masih saja terjadi di era kenormalan baru. Indonesia dapat mencontoh Malaysia yang memiliki pusat koordinasi dan komando siber nasional (NC4) yang di dalamnya terdiri dari unit-unit yang menangani *Critical National Information Infrastructure* (CNII). CNII bertugas untuk melaporkan, menyebarkan informasi, dan mengambil tindakan untuk melindungi sistem TIK penting mereka. Unsur-unsur di dalam CNII ini terdiri dari berbagai sektor badan publik dan swasta, seperti: layanan pemerintah, perbankan dan keuangan, transportasi, keamanan dan pertahanan, layanan darurat, informasi dan komunikasi, pelayanan kesehatan, air, energi, serta pangan dan pertanian. Indonesia dapat pula mengembangkan ekosistem kerja sama lintassektor melalui model di Inggris Raya dan negara-negara Eropa lainnya, yaitu menggunakan organisasi independen nonprofit bernama ISACs.

4) Meningkatkan kesadaran dan kapasitas SDM terkait keamanan siber

Untuk meningkatkan *security awareness* di Indonesia, maka Kementerian Kominfo, bersama dengan BSSN, Bank Indonesia (BI), dan Otoritas Jasa Keuangan (OJK), melakukan literasi dan sosialisasi dalam bentuk *webinar* dan iklan layanan masyarakat di berbagai media untuk

memberikan pemahaman masyarakat mengenai bentuk serangan siber yang sering muncul selama pandemi Covid-19 dan cara mengatasinya, khususnya di sektor keuangan. Dari sisi penyelenggara industri, BSSN juga berupaya memberikan fasilitasi pendampingan terhadap berbagai perusahaan di semua sektor untuk meningkatkan standar keamanan sistem informasi dan jaringan mereka. Pemerintah juga perlu serius mengatasi masalah rendahnya kapasitas Sumber Daya Manusia (SDM) di bidang keamanan siber. Hal ini disebabkan masih kurangnya anak muda yang tertarik memasuki profesi tersebut karena belum ada jalur karir dan pelatihan yang memadai dalam bidang keamanan siber.

KESIMPULAN

Pandemi virus Covid-19 telah mendorong percepatan transformasi digital sehingga menyebabkan terjadinya disrupsi di segala bidang. Tingginya aktivitas masyarakat yang melibatkan teknologi digital menjadi sasaran empuk kejahatan dunia siber. Ancaman serangan siber di masa kenormalan baru tidak hanya semakin meningkat jumlahnya tetapi juga semakin lihai dalam mendekati korbannya. Tidak hanya menggunakan teknologi, pendekatan secara *social engineering* juga dilakukan untuk dapat menyusup ke data pribadi calon korbannya. Melalui *benchmarking* dengan metode analisis Narrative Policy Framework (NPF), teridentifikasi bahwa karakter *hero* yang diwakili oleh regulasi perlindungan data pribadi yang komprehensif telah lama digunakan oleh Inggris Raya dan Malaysia. Karakter *hero* di Indonesia tampaknya belum terlalu dominan karena ada *villain* yang hadir dalam bentuk ketiadaan regulasi terpadu untuk perlindungan data pribadi dari ancaman serangan siber. Dengan *victim* yang sama yaitu keamanan data pribadi dan data pelaku industri, maka Indonesia perlu mengambil langkah-langkah sebagai berikut: 1) mempercepat pengesahan RUU Perlindungan Data Pribadi, (2) menyediakan regulasi khusus yang menangani keamanan siber dan kejahatan kriminal siber, (3) membangun ekosistem penanganan keamanan siber lintassektor, (4) meningkatkan kesadaran dan kapasitas SDM terkait keamanan siber.

UCAPAN TERIMA KASIH

Ucapan terima kasih yang setinggi-tingginya saya sampaikan kepada beberapa institusi, yaitu institusi saya, Kementerian Komunikasi dan Informatika (Kominfo), yang telah memberikan kesempatan kepada penulis untuk memperdalam ilmunya sebagai bentuk pengabdian penulis kepada bangsa dan negara, juga terima kasih dan penghormatan kepada Badan Siber dan Sandi Negara (BSSN), serta Badan Intelijen Negara (BIN) sebagai garda terdepan terhadap penanggulangan serangan siber di Indonesia. Penulis juga tak lupa mengucapkan terimakasih kepada Bapak Adis dan Ibu Palupi selaku dosen di UI atas arahan dan bimbingannya selama proses penulisan.

DAFTAR PUSTAKA

Ardiyanti, Handrini. 2014. “Cyber-Security dan Tantangan Pengembangannya di Indonesia”. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional.* Vol.5 No. 1.

Bank Indonesia. 2018. "Hasil Survei BI Tahun 2018". *Seminar Daring Lindungi Data Pribadimu Dari Kejahatan Pembajakan One Time Password (OTP).* Departemen Pengembangan UMKM dan Perlindungan Konsumen, bahan tayang.

Björck F., Henkel M., Stirna J., Zdravkovic J. 2015. "Cyber Resilience – Fundamentals for a Definition". In: Rocha A., Correia A., Costanzo S., Reis L. (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing.* Vol 353. Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31.

Christensen, Clayton M., Rory McDonald, Elizabeth J. Altman, and Jonathan E. Palmer. 2018. "Disruptive Innovation: An Intellectual History and Directions for Future Research". Special Issue on Managing in the Age of Disruptions. *Journal of Management Studies*. Vol.55. No.7.

Dewi Rosadi, Sinta. 2015. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional.* Bandung: Refika Aditama.

FireEye. 2020. *APT41, Double Dragon, a dual espionage and cyber crime operation.* Special Report. https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html. Diakses 10 November 2020.

French, K., Shanahan, E. A., et.al. 2017."Narrative Frames and Settings in Policy Narratives". *The 3rd International Conference On Public Policy. The Lee Kuan Yew School of Public Policy (NUS),* Singapore.

Freeman, Mark and Ert, Van Gilbran. 2004. *International Human Rights Law.* Toronto, Canada.

Greenleaf, Graham. 2014. *Asian Data Privacy Laws.* Oxford: Oxford University Press.

Goestsch, David Goestsch and Davis, Stanley B. 1997. *Introduction to total quality : quality management for production, processing, and services.* New Jersey : Prentice Hall.

H. Lallie, L. Shepherd, J. Nurse et.al. 2020. "Cyber Security in The Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." I*nternational Journal for Research in Applied Science and Engineering Technology.* 10.22214/ijraset.2020.31216. Vol.8.

International Business Machines (IBM). 2020. COVID-19 Cyberwar: How to Protect Your Business. *Research Insights.*

Interpol General Secretariat. 2020. *Cyber Crime: Covid-19 Impact.* Lyon, France.

Jones, M.D., Shanahan, E.A., & McBeth, M.K. 2014*. "*Introducing the Narrative Policy Framework*".* dalam M.D. Jones, E.A. Shanahan, & M.K. McBeth (Eds.), *The Science of Stories: Applications of Narrative Policy Framework*. New York, NY: Palgrave MacMillan.

Kasali, Rhenald. 2017. *Disruption.* Jakarta: PT Gramedia Pustaka Utama.

Kurniawan, Sigit. 2020. *Kondisi Keamanan Siber Indonesia.* Badan Siber dan Sandi Negara (BSSN), bahan tayang.

McGuire, Mike, and Dowling, Samantha. 2013. *Cyber Crime: A Review of Evidence.* Research Report 75, Chapter2. Home Office.

Caroell, Noel and Conboy, Kieran. 2020. *"*Normalising the new normal: Changing Tech-Driven Work Practices Under Time Pressure*". International Journal of Information Management 55*.

Ochs, Thomas, and Ute Riemann. *Industry 4.0: How to manage transformation as the new normal.* The Palgrave Handbook of Managing Continuous Business Transformation. Palgrave Macmillan, London, 2017. 245-272.

Ozdemir, Vural, and Hekim, Nezih. 2017. "Birth of Industry 5.0: Making Sense og Big Data with Artificial Intelligence, The Internet of Things and Next Generation Technology Policy.*" OMICS: A Journal of Integrative Biology*. http://mc.manuscriptcentral.com/omics.

Radanliev, Petar, David De Roure, and Max Van Kleek. 2020. *"*Digitalization of COVID-19 pandemic management and cyber risk from connected systems". https://iot.ieee.org/newsletter/may-2020/digitalization-of-covid-19- pandemic-management-and-cyber-risk-from-connected-systems.

Rahmawati, Ineu. 2017. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense". *Jurnal Pertahanan & Bela Negara.* Vol.7.No.2.

Ramli, Kalamullah. 2020. *Cerdas Bertelekomunikasi Untuk Menghindari Fraud: Tinjauan Kebijakan dan Regulasi.* The Center for Cyber Awareness and Resilience (id-CARE). Unversitas Indonesia.

Salahudin.2019. *Filosofi dan Metodologi Narrative Policy Framework (NPF).* Universitas Muhamadiyah Yogyakarta.

S. Hakak, W. Z. Khan, M. Imran, K. R. Choo and M. Shoaib. 2019. "*Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies.*" in *IEEE Access,* Vol. 8, pp. 124134-124144, 2020, doi: 10.1109/ACCESS.2020.3006172.

Sunkpho, Jirapan., Sarawut Ramjan, Chaiwat Ottamakorn. 2018. *"*Cybersecurity Policy in ASEAN Countries*". Information Institute Conferences, Las Vegas, NV, March 26-28*.

United Nation Office on Drug and Crime (UNODC). 2020. *COVID-19: Cyber Threat Analysis.*

Warren, Samuel and Brandeis, D, Louis. 1890.*"The Right to Privacy."* Harvard Law Review. Vol.4 No.5

WHO. 2020. Coronavirus Disease (COVID-19) Dashboard. https://covid19.who.int. diakses 15 November 2020.